IN THE CLAIMS

Please amend the claims as follows:

Claim 1 (Currently Amended): An information recorder for recording information to a recording medium, the apparatus comprising:

a transport stream processing means for appending an arrival time stamp (ATS) to each of discrete transport packets included in a transport stream; and

a cryptography means for generating a block key for encrypting a block data including more than one transport packet each having the appended arrival time stamp (ATS) from a block seed which is additional information unique to the block data and including the arrival time stamp (ATS), and encrypting each block data with the block key thus generated;

the data encrypted by the cryptography means being recorded to the recording medium; and

wherein the cryptography means generates a title-unique key from a key stored in the information recorder, disk ID and a title key unique to data to be recorded to the recording medium, and

generates the block key from the title-unique key and block seed.

Claim 2 (Original): The apparatus according to claim 1, wherein the cryptography means generates the block key for encrypting the block data from a block seed which is additional information unique to the block data and including the arrival time stamp (ATS) appended to a leading one of the plurality of transport packets included in the block data.

Claim 3 (Canceled).

Claim 4 (Original): The apparatus according to claim 1, wherein the cryptography means generates a disc ID being a recording medium identifier unique to a recording medium and a title key unique to data to be recorded to the recording medium, and stores them into the recording medium.

Claim 5 (Original): The apparatus according to claim 1, wherein the block seed includes copy control information in addition to the arrival time stamp (ATS).

Claim 6 (Original): The apparatus according to claim 1, wherein the cryptography means encrypts, with the block key in the encryption of the block data, only data included in the block data and excluding data in a leading area including a block seed of the block data.

Claim 7 (Original): The apparatus according to claim 1, wherein the cryptography means generates a title-unique key from a master key stored in the information recorder, disc ID being a recording medium identifier unique to a recording medium and a title key unique to data to be recorded to the recording medium, takes the thus-generated title-unique key as a key for an encryption function, places the block seed into the encryption function, and outputs a result of the placement as a block key.

Claim 8 (Original): The apparatus according to claim 1, wherein the cryptography means generates a title-unique key from a master key stored in the information recorder, disc ID being a recording medium identifier unique to a recording medium and a title key unique

to data to be recorded to the recording medium, places the title-unique key thus generated and block seed into a one-way function, and outputs a result of the placement as a block key.

Claim 9 (Currently Amended): The apparatus according to claim 1, wherein the cryptography means generates a device-unique key from any of an LSI key stored in an LSI, large scale integrated circuit, included in the cryptography means, device key stored in the information recorder, medium key stored in the recording medium and a drive key stored in a drive unit for the recording medium or a combination of these keys, and generates a block key for encrypting the block data from the device-unique key thus generated and block seed.

Claim 10 (Original): The apparatus according to claim 1, wherein the cryptography means encrypts block data with the block key according to a DES algorithm.

Claim 11 (Original): The apparatus according to claim 1, further comprising an interface means for receiving information to be recorded to a recording medium, and identifying copy control information appended to each of packets included in the transport stream to judge, based on the copy control information, whether or not recording to the recording medium is allowed.

Claim 12 (Original): The apparatus according to claim 1, further comprising an interface means for receiving information to be recorded to a recording medium, and identifying 2-bit EMI (encryption mode indicator) as copy control information to judge, based on the EMI, whether or not recording to the recording medium is allowed.

Claim 13 (Currently Amended): An information player for playing back information from a recording medium, the apparatus comprising:

a cryptography means for decrypting encrypted data recorded in the recording medium by generating a block key for decrypting encrypted data of a block data having an arrival time stamp (ATS) appended to each of a plurality of transport packets from a block seed which is additional information unique to the block data and including the arrival time stamp (ATS), and decrypting each block data with the block key thus generated; and

a transport stream processing means for controlling data output on the basis of the arrival time stamp (ATS) appended to each of the plurality of transport packets included in the block data having been decrypted by the cryptography means; and

wherein the cryptography means generates a title-unique key from a key stored in the information recorder, disk ID and a title key unique to data to be recorded to the recording medium, and

generates the block key from the title-unique key and block seed.

Claim 14 (Original): The apparatus according to claim 13, wherein the cryptography means generates the block key for decrypting the block data from a block seed which is additional information unique to the block data and including the arrival time stamp (ATS) appended to a leading one of the plurality of transport packets included in the block data.

Claim 15 (Canceled).

Claim 16 (Original): The apparatus according to claim 13, wherein the block seed includes copy control information in addition to the arrival time stamp (ATS).

Claim 17 (Original): The apparatus according to claim 13, wherein the cryptography means decrypts, with the block key, only data included in the block data and excluding data in a leading area including a block seed of the block data.

Claim 18 (Original): The apparatus according to claim 13, wherein the cryptography means generates a title-unique key from a master key stored in the information player, disc ID being a recording medium identifier unique to a recording medium and a title key unique to data to be recorded to the recording medium, takes the thus-generated title-unique key as a key for an encryption function, places the block seed into the encryption function, and outputs a result of the placement as a block key.

Claim 19 (Original): The apparatus according to claim 13, wherein the cryptography means generates a title-unique key from a master key stored in the information player, disc ID being a recording medium identifier unique to a recording medium and a title key unique to data to be recorded to the recording medium, places the title-unique key thus generated and block seed into a one-way function, and outputs a result of the placement as a block key.

Claim 20 (Currently Amended): The apparatus according to claim 13, wherein the cryptography means generates a device-unique key from any of an LSI key stored in an LSI, large scale integrated circuit, included in the cryptography means, device key stored in the information player, medium key stored in the recording medium and a drive key stored in a

drive unit for the recording medium or a combination of these keys, and generates a block key for decrypting the block data from the device-unique key thus generated and block seed.

Claim 21 (Original): The apparatus according to claim 13, wherein the cryptography means decrypts block data with the block key according to a DES algorithm.

Claim 22 (Original): The apparatus according to claim 13, further comprising an interface means for receiving information to be recorded to a recording medium, and identifying copy control information appended to each of packets included in the transport stream to judge, based on the copy control information, whether or not playback from the recording medium is allowed.

Claim 23 (Original): The apparatus according to claim 13, further comprising an interface means for receiving information to be played back from a recording medium, and identifying 2-bit EMI (encryption mode indicator) as copy control information to judge, based on the EMI, whether or not playback the recording medium is allowed.

Claim 24 (Currently Amended): A method for recording information to a recording medium, the method comprising the steps of:

appending an arrival time stamp (ATS) to each of discrete transport packets included in a transport stream; and

generating a block key for encrypting a block data including more than one transport packet each having the appended arrival time stamp (ATS) from a block seed which is

additional information unique to the block data and including the arrival time stamp (ATS), and encrypting each block data with the block key thus generated;

the data encrypted in the cryptographic step being recorded to the recording medium;

a title-unique key is generated from a key stored in the information recorder, disc ID and a title key unique to data to be recorded to the recording medium, and the block key is generated from the title-unique key and block seed.

Claim 25 (Original): The method according to claim 24, wherein in the cryptographic step, the block key for encrypting the block data is generated from a block seed which is additional information unique to the block data and including the arrival time stamp (ATS) appended to a leading one of the plurality of transport packets included in the block data.

Claim 26 (Canceled).

Claim 27 (Original): The method according to claim 24, further comprising the step of generating a disc ID being a recording medium identifier unique to a recording medium and a title key unique to data to be recorded to the recording medium, and storing them into the recording medium.

Claim 28 (Original): The method according to claim 24, wherein in the cryptographic step, only data included in the block data and excluding data in a leading area including a block seed of the block data is encrypted with the block key in the encryption of the block data.

Claim 29 (Original): The method according to claim 24, wherein in the cryptographic step, a title-unique key is generated from a master key stored in the information recorder, disc ID being a recording medium identifier unique to a recording medium and a title key unique to data to be recorded to the recording medium, the title-unique key thus generated is taken as a key for an encryption function, the block seed is placed into the encryption function, and a result of the placement is outputted as a block key.

Claim 30 (Original): The method according to claim 24, wherein in the cryptographic step, a title-unique key is generated from a master key stored in the information recorder, disc ID being a recording medium identifier unique to a recording medium and a title key unique to data to be recorded to the recording medium, the title-unique key thus generated and block seed are placed into a one-way function, and a result of the placement is outputted as a block key.

Claim 31 (Original): The method according to claim 24, wherein in the cryptographic step, a device-unique key is generated from any of an LSI key stored in an LSI, large scale integrated circuit, included in the cryptography means, device key stored in an information recorder, medium key stored in the recording medium and a drive key stored in a drive unit for the recording medium or a combination of these keys, and a block key for encrypting the block data is generated from the device-unique key thus generated and the block seed.

Claim 32 (Original): The method according to claim 24, wherein in the cryptographic step, the encryption of block data with the block key is made according to a DES algorithm.

Claim 33 (Original): The method according to claim 24, further comprising the step of identifying copy control information appended to each of packets included in the transport stream to judge, based on the copy control information, whether or not recording to the recording medium is allowed.

Claim 34 (Original): The method according to claim 24, further comprising the step of identifying 2-bit EMI (encryption mode indicator) as copy control information to judge, based on the EMI, whether or not recording to the recording medium is allowed.

Claim 35 (Currently Amended): A method for playing back information from a recording medium, the method comprising the steps of:

generating a block key for decrypting encrypted data in a block data having an arrival time stamp (ATS) appended to each of a plurality of transport packets from a block seed which is additional information unique to the block data and including the arrival time stamp (ATS), and decrypting each block data with the block key thus generated; and

processing a transport stream processing means to control data output on the basis of the arrival time stamp (ATS) appended to each of the plurality of transport packets included in the block data having been decrypted in the decrypting step;

wherein in the decrypting step, a title-unique key is generated from a key stored in the information player, disc ID and a title key unique to data to be recorded to the recording medium, and the block key is generated from the title-unique key and block seed.

Claim 36 (Original): The method according to claim 35, wherein in the decrypting step, the block key for decrypting the block data is generated from a block seed which is

additional information unique to the block data and including the arrival time stamp (ATS) appended to a leading one of the plurality of transport packets included in the block data.

Claim 37 (Canceled).

Claim 38 (Original): The method according to claim 35, wherein in the decrypting step, only data included in the block data and excluding data in a leading area including a block seed of the block data is decrypted with the block key in the encryption of the block data.

Claim 39 (Original): The method according to claim 35, wherein in the decrypting step, a title-unique key is generated from a master key stored in the information player, disc ID being a recording medium identifier unique to a recording medium and a title key unique to data to be recorded to the recording medium, the title-unique key thus generated is taken as a key for an encryption function, the block seed is placed into the encryption function, and a result of the placement is outputted as a block key.

Claim 40 (Original): The method according to claim 35, wherein in the decrypting step, a title-unique key is generated from a master key stored in the information player, disc ID being a recording medium identifier unique to a recording medium and a title key unique to data to be recorded to the recording medium, the title-unique key thus generated and block seed are placed into a one-way function, and a result of the placement is outputted as a block key.

Claim 41 (Original): The method according to claim 35, wherein in the decrypting step, a device-unique key is generated from any of an LSI key stored in an LSI, large scale integrated circuit, included in the cryptography means, device key stored in the information player, medium key stored in the recording medium and a drive key stored in a drive unit for the recording medium or a combination of these keys, and a block key for decrypting the block data is generated from the device-unique key thus generated and block seed.

Claim 42 (Original): The method according to claim 35, wherein in the decrypting step, the block data decryption with the block key is made according to a DES algorithm.

Claim 43 (Original): The method according to claim 35, further comprising the step of identifying copy control information appended to each of packets included in the transport stream to judge, based on the copy control information, whether or not playback from the recording medium is allowed.

Claim 44 (Original): The method according to claim 35, further comprising the step of identifying 2-bit EMI (encryption mode indicator) as copy control information to judge, based on the EMI, whether or not playback from the recording medium is allowed.

Claims 45-47 (Canceled).